## **Summer of Innovation, Requirements Team**

## **Air Force Research Laboratory, Wright Brothers Institute, Summer 2017**

General

1. A **reusable framework** is needed to support a broad class of autonomous ISR missions using unmanned assets —  including unmanned aircraft.
2. The framework must enable **distributed**, multi-agent **cooperative control** in a comms-denied environment.
3. The framework must be **modular**, must be **computationally efficient** and run on modest hardware, and must allow capabilities such as **mission planning**, path planning, and surveillance tasks to be **efficiently developed** and rapidly updated and replaced before the start of each ISR mission.
4. The framework must optimize tasks for mission-time efficiency.
5. The framework must ensure **safety** and **security**.
6. The framework must facilitate **formal verification and validation**.

Reviewed/Consolidated Reqs

1. 1-UxAS shall enable cooperative control
2. 2-UxAS shall support multiple agents
3. 3-UxAS shall be distributed
4. 25-UxAS shall operate when there is no comms
5. 4-UxAS shall operate in the presence of lost comms
6. 5-UxAS shall operate in the presence of denied comms
7. 6-UxAS shall be modular
8. 7-UxAS shall be computationally efficient
9. 8-UxAS will run on modest hardware, e.g., cell-phone sized processor
10. 35-UxAS shall allow tasks to be efficiently developed
11. 11-Example tasks include mission planning, path planning, and surveillance
12. 26-UxAS shall allow configurations to be rapidly modified before the start of a mission
13. 9-Configuration modification includes task update before the start of each mission
14. 27-update may mean that the component satisfies its contract in a new way
15. 10-Configuration modification includes task replacement before the start of a mission
16. 28-replace may mean that the contract has been changed and the configuration needs to be re-analyzed
17. 12-Configurations shall optimize tasks for mission-time efficiency
18. 13-Configurations shall ensure the safety of agents
19. 39-Safety includes collision avoidance, health monitoring, contingency planning (safe route home for lost comms)
20. 14-Configurations shall ensure security
21. 30-Security includes integrity & confidentiality of comms
22. 31-Security includes integrity & confidentiality of onboard data
23. 32-Security includes availability of computing resources
24. 34-UxAS shall facilitate formal verification and validation
25. 15-UxAS shall be employ a service-oriented architecture
26. 35-The service oriented architecture provides the basis for configurations
27. 16-Configurations shall ensure schedulability of tasks
28. 17-Configurations shall ensure timeliness of task execution
29. 33-Configurations shall ensure timeliness of message delivery within an asset
30. 18-Configurations shall guarantee non-interference amongst services under nominal hardware configurations
31. 19-Configurations shall provide time partitioning of services
32. 20-Configurations shall provide space partitioning of services
33. 21-Configurations shall provide resource partitioning of services
34. 22-For example, configurations will schedule direct-memory access
35. 23-Configurations shall provide a message-passing interface for inter-service communication
36. 24-Configurations shall provide a standard interface for all services

System-Level Properties

1. SYS1-For every Unique Automation Request, the system produces a response (which might be an error message).
2. SYS2-Every task included in a request should be in the response or an error should be produced.
3. SYS3-The system shall respect airspace constraints
4. SYS4-No path produced will intersect with a no fly zone.
5. SYS5-Vehicles should stay in Keep In Zones
6. SYS6-If there is a feasible assignment (mission solution), we should find it.
7. SYS7- If the process algebra relationship is valid (well-formatted), then we should adhere to it.
8. SYSA2-Vehicles altitudes are distinct and differ by at least X ft
9. SYS8-Vehicle altitudes shall not be changed during the mission
10. SYS10-The costs of tasks and mission are influenced by vehicle altitude
11. SYSA1-If a map update is sent by the user, that user will also determine when to force a replan (for the entire system).
12. SYS9-Assignment cost matrix coming out of route aggregator service should be #vehicles\* # task options + # vehicles\* (#task options)^2.
13. SYS10-Message IDs shall be unique system-wide throughout a mission
14. SYS11-Route planner shall be configured with vehicle configuration data before a route plan request is sent (or received)?
15. SYS12-Messages shall be received in the order in which they were sent
16. SYS13-The system shall propagate error messages to the final recipient
17. SYS14-For each request sent, a response (possible an error) is received and that response corresponds to that request.

Proposed Requirements

1. P2-The configuration shall report an error if an automation request is received but the requested resource has not been defined
2. P3-Resources include Tasks, Vehicles and Regions
3. P4-The configuration shall generate a UniqueAutomationRequest message if an AutomationRequest is received and the requested resource has been defined
4. P5-The configuration shall publish UniqueAutomationRequest messages in the order in which they are generated
5. P7-The configuration shall publish one UniqueAutomationRequest message and wait for a corresponding UniqueAutomationResponse message to be received
6. P8-The configuration shall publish the next UniqueAutomationRequest message immediately if there is no outstanding UniqueAutomationResponse message
7. P9-Optionally, the configuration shall publish the next UniqueAutomationRequest if the outstanding UniqueAutomationResponse message has not been received within a set time
8. P10-The configuration shall publish an AutomationResponse message in response to the corresponding AutomationRequest message when a corresponding UniqueAutomationResponse message is received
9. P11-The configuration shall ensure that only one AutomationRequest is executed at a time

RouteAggregator Requirements

1. RA1-The configuration shall create a unique RoutePlanRequest message for each vehicle ID in each RouteRequest message received
2. RA2-The configuration shall send each RoutePlanRequest message to the planners that are appropriate for the associated vehicle type
3. RA3-The configuration shall correlate RoutePlanReponses with RoutePlanRequests
4. RA4-The configuration shall send a RouteResponse message when all RoutePlanResponses are received for a particular RouteRequest

RoutePlannerVisibility Requirements

1. RPV1-The configuration shall generate a route for each pair of start and end locations specified in each RoutePlanRequest message received
2. RPV2-Route generation shall be efficient
3. RPV3-Route generation shall be responsive
4. RPV4-Routes shall be approximately distance optional
5. RPV5-Routes shall respect vehicle limitations
6. RPV6-Vehicle limitations include minimum turn radius constraints
7. RPV7-The configuration shall send a RoutePlanResponse message using return-to-sender addressing when a route has been generated for all pairs of start and end locations specified in the associated RoutePlanRequest message
8. RPV8-The configuration shall take environment and vehicle constraint information from appropriate inputs

Secure Communication Requirements

1. SR1-UxAS shall ensure communication is only between intended services.
2. SR2-UxAS shall ensure data is only accessible to services with appropriate authority.
3. SR3-UxAS communication channels shall be always avaiable to intended users.
4. SR4-UxAS will filter out garbage data from communication channels.
5. SR5-UxAS shall detect the authenticity of incoming messages.
6. SR6-UxAS will detect if an attacker resends an old message.
7. SR7-UxAS will encrypt communications.
8. SR8-UxAS shall verify received messages are from a source authorized to send the given message type.